通过分层安全框架管理GPO

作者：Alvaro Vitta，Quest的首席解决方案顾问

简介

组策略为Microsoft Active Directory环境中的操作系统、应用程序和用户设置提供集中式管理与配置。在某种程度上，组策略控制用户可以或不能在计算机系统上执行哪些操作。它施行密码复杂性系统以避免用户选择过于简单的密码，阻止或允许身份不明的用户从远程计算机连接到网络共享，并限制访问某些文件夹。这样一套配置称为组策略对象(GPO)。

虽然GPO的设计目的是为了简化IT操作和跨Active Directory环境提供集中式安全策略，但是与任何其他强大的系统一样，GPO也会遭到滥用或侵入，以规避安全控制和获取敏感数据的访问权限。一些大中型企业跨大范围分布式环境部署了数百甚至数千个GPO，这不仅会产生巨大的内部威胁，还会暴露大量表面攻击区域（在未提供适当补偿安全控制的情况下）。

本白皮书介绍了在未提供适当安全控制的情况下GPO如何遭到滥用或侵入，并解释了如何实施分层安全基础架构，便于您检测、阻止对GPO的未经授权访问并发出相应警报。

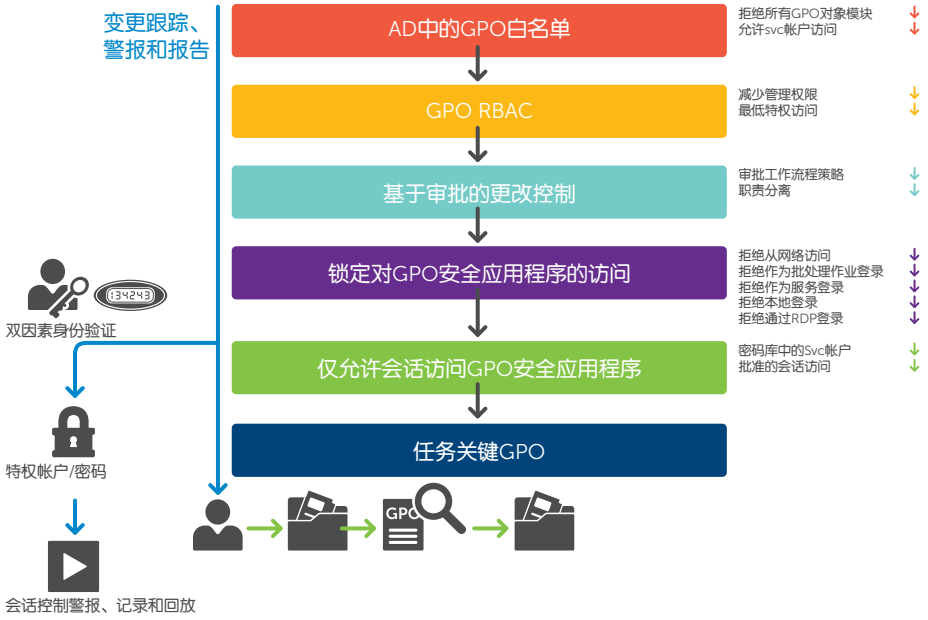

图1. GPO分层安全框架

55 %的安全事件是由内部人员滥用其访问权限而导致的。[1]

GPO权限侵入

Sam Smith是一家生产企业新聘请的IT管理员，需要为基于Windows的数据库服务器（包含机密客户信息的敏感SQL数据库）安装修补程序。Sam是域管理员，无法登录到此SQL服务器，因为GPO（**拒绝本地登录**）已被专门设置为阻止域管理员登录到这个含个人客户详细信息的特定SQL服务器。在周六的变更管理期间，他未得到修补程序安装的审批，也没有注意相应规定，而是决定更改GPO设置“**拒绝本地登录**”，以允许自己访问此服务器。他停用了阻止管理员登录的GPO，然后登录服务器以安装修补程序。登录后，他非常好奇，决定偷看一些敏感客户数据，甚至还将部分此类信息复制到单独的文件夹中。随后，他将GPO改回到了原始设置。由于本机安全日志不会跟踪GPO设置更改，因此，直到六周后，公司进行数据库审核时，才发现并举报了这一未经授权访问。

此类安全漏洞是如何出现的?

很不幸，类似事件（无论性质是意外还是恶意）发生的频率比您想象的还要频繁。由于GPO安全权限设计的方式，任何域管理员都可以修改任何GPO安全设置（即使此类设置应该会阻止此类非常人员执行某些任务）。此外，由于本机安全日志不会跟踪GPO设置更改，因此，即使您使用的是安全信息和事件管理(SIEM)解决方案，监控此类GPO设置更改发生的时间也是不可能的。另外，您无法阻止此类事件以后再次发生，因为您没有办法掌握更改的确切GPO设置（更改前后的值），而且您的域管理员可以随意更改GPO设置。

分层安全框架

阻止如上文所述的数据泄露及其他多种类型的数据泄露（就此而言）的一种方式是，确保分层方法的安全。您需要一套紧密结合的安全控制，便于管理员在获得授权的情况下更改GPO设置，同时阻止外部或内部资源（甚至域管理员）对其进行未经授权的更改。

以下安全层可以共同发挥作用，为管理任务关键GPO设置的访问权限提供适当的安全补偿控制：

- Active Directory中的GPO白名单
- GPO基于角色的访问控制(RBAC)
- 基于审批的更改控制
- 锁定GPO安全应用程序的访问权限
- 仅允许会话访问GPO安全应用程序

Active Directory中的GPO白名单

所有敏感GPO（如域范围内的GPO、域控制器GPO、任务关键应用程序GPO等）都会添加到Change Auditor for Active Directory等第三方安全应用程序（具有GPO白名单权限功能）的“保护列表”中。这款Windows安全解决方案的功能可支持实时权限白名单，并允许监控对GPO设置企图进行未经授权更改的行为。

只有特定“GPO服务帐户”（由有权更改GPO的第三方GPO（代理）安全解决方案（如GPOAdmin）使用）才会被列为有权修改最敏感的GPO。系统会自动拒绝其他所有帐户更改GPO（包括域管理员）。只有通过GPOAdmin界面才能进行授权更改，因为此界面可提供最低权限的访问模型和适当的GPO更改监管控制。使用GPO白名单安全应用程序可避免与未获得授权进行日常修改有关的风险。

GPO RBAC

虽然本机GPO权限的设计目的是为了向GPO授予权限，但有时这些权限会产生利益冲突。例如，域管理员组成员可以随意更改相同的GPO安全设置（其起初应该会阻止此成员执行某些任务）。因此，最好实施基于角色的访问控制模型，便于GPO权限从Active Directory扩展到其他环境，并由GPOAdmin等第三方GPO（代理）安全解决方案来控制。GPOAdmin是适用于GPO的生命周期管理解决方案。GPOAdmin可提供最低权限的访问模型，并允许您减少具有GPO设置过度访问权限的管理员数量。

基于审批的更改控制

建立GPO白名单和GPO RBAC模型后，您需要设置自动化流程以支持使用审批工作流程的职责分离，便于区分开GPO设置的修改人员与将GPO更改部署到生产环境的审批人员。这虽然看似很明显，但仍需要得到正式解决和实施。

锁定GPO安全应用程序的访问权限

当您使用第三方GPO安全应用程序（如Change Auditor for Active Directory和GPOAdmin）控制GPO更改时，此类应用程序就变得尤为关键。因此，锁定对此类安全解决方案的未经授权访问也就变得十分重要了。要添加此安全层，您只需将GPO安全策略添加到白名单中，然后将其应用到托管安全应用程序的服务器即可。请使用以下设置：

“拒绝作为批处理作业登录”、“拒绝从网络访问”、“拒绝作为服务登录”、“拒绝本地登录”和“拒绝通过RDP登录”

69 %的特权用户说，安全工具提供的事件信息不充分。[2]

分层安全基础架构可让您检测、阻止对GPO的未经授权访问并发出相应警报。

仅允许会话访问GPO安全应用程序

要为服务器管理员创建安全的访问权限，让其对第三方GPO安全应用程序执行常规维护任务，您提供的控制访问权限必须是在The Privileged Appliance and Modules (TPAM)等“跳转服务器”中通过加密远程桌面连接实现。双因素身份验证系统（如Quest Defender）也可以将此类服务器放在前端，以提供额外一层的安全保护。在跳转服务器（即增强设备）中，基于时间的会话得到相应审批人员的审批后，授权员工可以连接到第三方GPO安全应用程序服务器来执行具体的维护任务。所有会话操作都会得到记录并可以按需回放，以详细列出在服务器上执行的所有操作。

总结

很不幸，任何企业都会发生GPO安全事件（无论是意外事件还是恶意事件）。假定内置安全日志提供的信息不充分，而且本机权限的灵活性过低，则您所需的分层安全框架须具有第三方GPO安全解决方案的功能，以检测GPO安全事件、发出相应警报，并阻止此类事件将企业内有价值的数据至于危险境地。

关于作者

Alvaro Vitta是Quest Group的首席解决方案顾问，专门从事安全性方面的工作。Vitta一直在大型企业中为私人部门和公共部门的内部部署和基于云的平台评估、设计、测试及部署安全解决方案，而且在以下方面的从业经验长达15年：身份和访问管理、Active Directory及跨全球企业的监管、风险和合规性。Vitta持有行业认证，包括CISSP、CISSO、MCSE和ITIL。

[1] *“2015 Data Breach Investigations Report”（《2015年数据泄露调查报告》），Verizon，2015年4月，http://www.verizonenterprise.com/DBIR/2015*

[2] *“Privileged User Abuse and the Inside Threat”（《特权用户滥用与内部威胁》），Raytheon Company，2014年5月，http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_257010.pdf。*

关于QUEST

Quest可帮助我们的客户减少乏味的管理任务，便于他们专注于实现业务发展所需的创新任务。Quest®解决方案可扩展、经济实惠且易于使用，而且提供卓越的能效和工作效率。与Quest对加入全球社区以成为其创新队伍一员的邀请，以及确保客户满意度的坚定承诺相结合，Quest将继续加快交付更全面的解决方案，从而实现Azure云管理、SaaS、安全性、办公移动性和数据驱动的洞察力。

如果您对本材料的可能用途存有任何问题，请联系：

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

请访问我们的网站(www.quest.com)，了解有关地区和国际办事处的相关信息。